Review Article

iMedPub Journals
http://www.imedpub.com/

American Journal of Computer Science and Information Technology

2018
Vol.6 No.3:27

DOI: 10.21767/2349-3917.100027

Internet of Things Security Issues and Their Solutions with Blockchain Technology Characteristics: A Systematic Literature Review

Abid Sultan[1*], Muhammad Sheraz Arshad Malik[1] and Azhar Mushtaq[2]

[1]Department of Information Technology, Government College University Faisalabad, Bhakkar, Punjab, Pakistan

[2]Department of CS&IT, University Of Sargodha, Bhakkar Campus, Pakistan

[*]**Corresponding author:** Abid Sultan, Department of Information Technology, Government College University Faisalabad, Bhakkar, Punjab, Pakistan, E-mail: abidsultan006@gmail.com

Received date: July 29, 2018; **Accepted date:** August 20, 2018; **Published date:** August 31, 2018

Citation: Sultan A (2018) Internet of Things Security Issues and Their Solutions With Blockchain Technology Characteristics: A Systematic Literature Review. Am J Compt Sci Inform Technol Vol.6 No.3:27

Abstract

Since the beginning of crypto currency in 2008, blockchain technology rise as progressive technology. Despite the fact that blockchain began off as a core technology of Bitcoin, its utilization cases are growing to numerous fields such as, security of Internet of Things (IoT), banking sector, industries and medical etc. In recent years IoT has gained popularity due to its usage in smart homes and smart city projects around the world. Unfortunately, IoT devices possess limited computing power, low storage capability and network capacity therefore they are more prone to attacks than other endpoint devices such as cell phones, tablets, or PCs. This paper focus on significant security issues for IoT, security prerequisites for IoT alongside the current attacks and maps IoT security issues against existing solutions found in the literature. Blockchain technology can be a key empowering influence to take care of numerous IoT security issues. Finally describe the future work directions.

Keywords: Blockchain; IoT; Network security; Data security; LLNs

Introduction

In today's era technologies have revolutionized the living standard of our society. This is often because of innovation in communication and semiconductor technologies, which permit devices to be connected over a network and alter the way of connectivity between machines and humans. Such a trend is usually noted as Internet-of-Things (IoT).

With the fast rise of brilliant devices and high speed networks, the IoT has gained wide acceptance and fame because it uses the standard called low-power lossy networks (LLNs). These LLNs have the potential to use limited resource by consuming very low power [1,2]. The devices in IoT may be controlled remotely to perform the specified function. The data sharing among the devices takes place through the network that employs the Standard protocols of communication. The good connected devices or "things" vary from easy wearable accessories to huge machines which contains detector (Sensor) chips.

According to International Data Corporation (IDC) report IoT will be implemented almost in every filed such as Industry, Government, and Consumer Sectors. Moreover, 20% of IoT organizations will use basic level services of Blockchain. Furthermore, almost 75% of all IoT manufactures will improve the security capabilities thus making them more attractive for buyers [3].

However, as IoT rising the connectivity is increasing, and also the computing infrastructure can become additional complicated. This complication can give a rise to vulnerabilities for the cyber-attacks. In IoT the physical devices are placed in unsecured environments which could be defenseless from hackers thus giving them the opportunity to alter the information that travel over the network. Therefore, device authorizations and information root would be a vital issue.

Blockchain is a sequence of blocks that hold all transaction record in a blockchain network. As described in **Figure 1** each block contains block header and block body. Block header contains the following:

- **Block version** which indicate the software version and validation rules.
- **Merkle Tree root hash** represents the hash value of transaction and summary of all transaction.
- **Time stamp** consists of current universal time since January 1970.
- **N-Bits** define the number of bits required for transaction verification.
- **Nonce** holds any 4 byte number which starts from 0 and increase for every hash of the transaction.
- **Parent block hash** contains the hash value which indicates the previous block.

Block body covers all transaction records. Maximum number of transaction depends upon the block size [4-12]. Blockchain technology referred as a public ledger and all completed

transactions are recorded in a list of blocks. This chain of blocks grows as new blocks are added to chain continuously. Public key cryptography and distributed consensus algorithms are implemented for the user security.

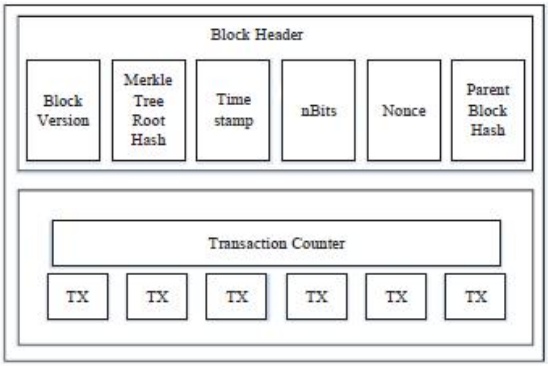

Figure 1: Block Architecture [13]

The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these characteristics, blockchain can greatly save the cost and increases the effectiveness [13]. This paper is ordered as follows. Section II covers the Blockchain Properties whereas section III highlights its characteristics. Different security necessities and issues are covered in section IV and section V provides the solution of security issues using blockchain. Finally in Section VI conclusion and future work is presented. **Table 1** represent the issues that are faced in IOT network and which Blockchain feature solve them.

Blockchain

Blockchain working

Working of blockchain consists of the fowling steps. Nodes communicate with the blockchain network *via* a combination of private and public keys. They use their private key to digitally sign their own transactions and then can access the network *via* their public key. Each signed transaction is broadcast by a node that makes the transaction [4]. The transaction is then verified by all nodes within the blockchain network except the node that makes the transaction. During this step, any invalid transaction is discarded. It's known as verification.

Every node collects the transactions that are valid during a sure time into a block and implements a proof-of-work to find a nonce for its block. Once a node finds a nonce, it broadcasts the block to all participating nodes. This is a method known as mining [5]. Each node chose a block publicized for the first time and confirm that the block (a) holds legal transactions, and (b) mentions through hash the accurate previous block on their blockchain. If that is the situation, they added the block to their blockchain and apply the transactions it holds to bring up-to-date their blockchain. If that is not the case, the projected block is rejected. This terminates the existing mining round [4].

Verification

Blockchain technology ensures the elimination of the duplication issues, with the assistance of public-key cryptography, whereby every node is assigned a non-public key that is shared with all alternative nodes [6]. Once a signed transaction is broadcast by a node that makes the transaction, all receiving nodes verify the transaction by decrypting a signature with a public key of an initializing node. If a signature verification result's true, the signed dealings is verified that the initializing node isn't modified.

Proof-of-Work

The proof-of-work (**Figure 2**) contains the process of scanning for a value that hashed with Secure Hash Algorithm 256. The typical work needed is exponential within the variety of zero bits needed and confirmed by running hash algorithm. In an exceedingly blockchain network, all nodes implement the proof-of-work for every mining process by increase a nonce within the block till a value is founded that offers the block's hash desired bits.

Once the system unit effort has been spent to satisfy the proof-of-work, the block can't be modified until not redoing the work. Blockchain feature distributed IoT information management can provide users the choice of sharing the information with third party entities. The target, is to supply a distributed information access model for IoT, that ensures that user-data isn't assigned to centralized entities or corporations [5].

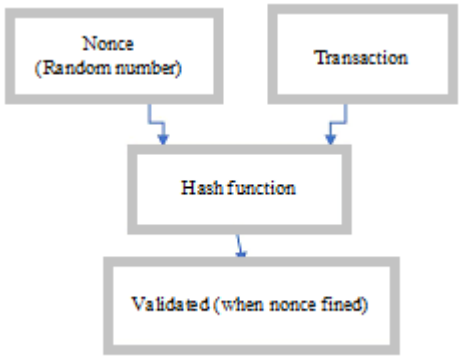

Figure 2: Proof-of-Work

Characteristics of Blockchain

Decentralization

In centralized transaction processing environment, each transaction needs to be validated through the centralized trusted party (e.g., banking system), that resulting to the cost and the performance decrees at the central point. With respect to the centralized IOT model, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data integrity and consistency [13].

Persistency

Once a transaction record is validated by a miner node (special nodes that validate the transaction) in a blockchain network its copy is broadcast on the entire network and that record is not deleted or rollback from entire blockchain [13].

Anonymity

In Blockchain nodes interact with the network using public key that use to addresses the node on entire blockchain network but not acknowledge the real identities of the user [13].

Security

Blockchain use the asymmetric cryptographic technique to secure the entire network. Asymmetric or public key cryptography contain 2 keys one public key and second private key. Public key is used by the node to addresses in blockchain network and private key is use by the node to signs the transaction that it initiates. Other nodes use their public key and compare it after hashing to their signature for checking the initiator node identification.

Scalability or more addressing space

Blockchain contains 160-bit address space where IPv6 address has 128-bit address space, A Blockchain address is 20 bytes or 160-bit hash of the general public key generated by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain have 4.3 billion more Addresses over IPv6 [9].

Resilient backend

Every distributed node within the blockchain IOT network maintains a replica of the whole ledger. This helps in safeguarding the network form any potential failures and attacks [11].

High efficiency

Since the transaction removes the involvement of the third party and may proceed in Low-trust condition, the number of your time spent is obviously decrees whereas the efficiency is clearly increases [12].

Transparency

Changes made to public blockchain network are publicly viewable by all participants in the network. Moreover, all transactions are immutable, meaning they cannot be altered or deleted [10].

Smart contract

Smart contract is one of the most efficient aspects of the Ethereum introduced by Nick Szabo in 1994 [8]. Many programming languages are supported by Ethereum such as Solidity. Solidity is the most widespread used language and compiler. Using smart contract programs are written in which access rights and different policies are defined [14].

Security Necessities for IoT or Issues

Data privacy

Because of a diversified integration of services and network the data recorded on a device is vulnerable to attack by compromising nodes existing in associate IoT network. Moreover attacker Access the data without owner permission.

Data integrity

In centralized client server model the attacker may gain unauthorized access to the network and change the original data or information and forward it. For example, Alice sends data to Bob. Watson the middle guy might get data first and forward the data after modification.

Third party

Data collected in centralized environment is stored and controlled by a third centralized entity that may miss use this data or provide it to someone else.

Trusted data origin

In IOT environment it is difficult to know generated data come from which device that is stored in the entire network and can be altered by anyone.

Access control

Access control is one off the main issue in IoT network. To define which node have the right to access and perform different function in entire IOT network may be difficult.

Single points of failure

Continuous growth of centralized networks for the IoT based infrastructure could expose single-points-of-failure. Because all data of entire network store and verified by a central authority. If the central point is fail or down the whole network is down.

Scalability

Internet of thing connects a large numbers of sensors and other devices for information sharing and a large number of applications *via* internet. It challenges the structure and the rapid growth of the system to meet scalability.

Blockchain Solutions for IOT

Data integrity

Blockchain is a peer-to-peer network in which all nodes have same copy of records. When a transaction is initiated, initiator node signs the transaction with its private key and sends to other nodes for validation. All other miner nodes take part in validation process and try to find nonce. The node which finds the nonce first has the right to validate and get reward. Moreover, it will broadcast it to all other nodes of entire

network. Once the record is loaded in blockchain it cannot be modify Rollback or deleted [11].

Data privacy

Consortium blockchain used to provide data privacy in a blockchain network. As in **Figure 3** all nodes of entire network that are used for a particular purpose are combined together to form a private network/Sidechain. Each sidechain is responsible to manage its own IOT data. Nodes that are participant of one Sidechain are not take part in the validation process of other Sidechain. In order access the data of consortium blockchain network requestor node first need to register and became part of that Sidechain network than make access request. Consortium blockchain have access control and prevent from unauthorized access [7].

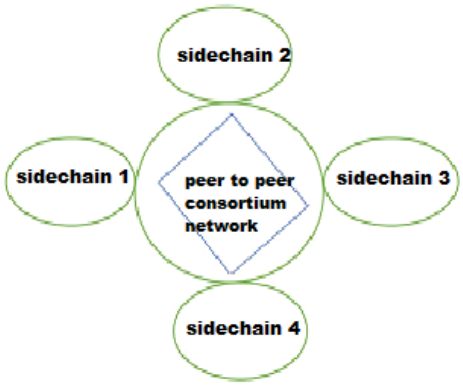

Figure 3: Consortium blockchain network

Addressing space

Blockchain contains a 160-bit address, While IPv6 address has 128-bit address Blockchain have 4.3 billion Addresses than IPv6 thus providing more addressing spacing than IPV6 address [9].

Trusted accountability

Every operations record must be uploaded to the blockchain network. This gives every operation an identity and each operation is traceable. When an abnormal behavior is detected entity send to origin for additional investigation [11].

Fault tolerance

Decentralized devices are less likely to fail accidentally because they rely on many separate components. Blockchain is point-to-point decentralizing network, in it every device has same copy of record that's why failure of a single node has not effect on the network. So, blockchain prevent from single point of failure.

Trusted data origin

In order to track data in blockchain network a unique id is assigned to each IoT devices. Data collected from a device is associated with its id and after calculating a hash on data submit to the entire network for high security [11].

Removing third-party risks

Blockchain technology makes the devices capable of performing operations without the intermediary or third party, thus making it risk free from third party [10].

Access control

Smart contract is one of the most efficient aspects of the Ethereum introduced by Nick Szabo in 1994 [8]. Using smart contract programs for blockchain are written in which access rights and different policies are defined. For example, a rule is set when meter reach at 135 KW devices are enter in energy saving mode.

Conclusion

IoT are most immerging technology with rise of high speed network and intelligent network devises but IoT devices are more prone to attack and unable of protecting themselves. In this paper we discuss different properties and characteristics of blockchain network such as POW, decentralization, persistency and network scalability. This paper aims to discuss different problems of the IOT devices (data integrity, access control and privacy etc.) and present possible blockchain network solutions proposed in the literature. Future work Some IoT devices are in openly reachable areas and actually below the control of an opponent, how can blockchain be used to assure the safety and confidentiality of the information kept in the device? How blockchain can decrease the option of the hardware and software of an IoT device from being compromised if the device is accessible to everyone? Under the narrow source, what is the best cost-efficient way to use blockchain based safety clarifications? Instead of providing different approaches for securing IoT, the blockchain systems are also prone to attack. The Validation mechanism hashing may be compromised, that allow the attacker to miss use the blockchain.

IOT Issues	Blockchain Characteristics							
	Decartelization	Persistency	Anonymity	Scalabilityor	Resilient	High efficiency	Transparency	Smart contract
Data Privacy	✓		✓	✓				✓
Data Integrity	✓	✓		✓				✓
Third party	✓				✓	✓		
Trusted Data Origin	✓	✓					✓	
Access control						✓	✓	✓
Single Points of Failure	✓				✓	✓		
Scalability				✓				

Table 1: IOT issues and Blockchain characteristics that solve them

References

1. Atzori L, Iera A, Morabito G (2010) the internet of things: A survey, Comput Netw 54: 2787-2805.
2. Giusto D, Iera A, Morabito G, Atzori L (2014) the Internet of Things: 20thTyrrhenianWorkshoponDigital Communications, Springer Publishing Company, Incorporated.
3. IDC, Future Scape (2017): Worldwide Internet of Things.
4. Christidis K, Devetsikiotis M (2016) Blockchains and Smart Constracts for the Internet of Things, IEEE Access 14: 2292-2230.
5. Nakamoto S (2008) Bitcoin: A Peer-to-Peer ElectronicCashSystem, https://bitcoin.org/bitcoin.pdf.
6. Pilkington M (2016) Blockchain technology: Principle and applications, Research Handbook on Digital Transformations.
7. https://www.researchgate.net/publication/32083144
8. Gord M (2016) Smart Contracts Described by Nick Szabo 20 Years ago NowBecoming Reality, Bitcoin Magazine.
9. Antonopoulos AM (2014) Mastering Bitcoin: Unlocking Digital Crypto-Currencies, 1st Edition, and O'Reilly Media.
10. http://www.techracers.com/blockchain-key-features
11. https://www.researchgate.net/publication/320339062
12. The IoT electric business model: Using blockchain technology for the internet of things.
13. https://www.researchgate.net/publication/318131748
14. Ethereum Frontier Guide, https://ethereum.gitbooks.io/frontier-guide,accessed2016 /10/31